

REMARKS

Claims 1, 3, 5, 7-8, 10, 13-15, 17, and 21 are pending and at issue in the above identified patent application. Of the claims at issue, claims 1, 8, and 15 are independent. In view of the following remarks, reconsideration and allowance of the application are respectfully requested.

The Rejections under 35 U.S.C. § 103

The claims were rejected as being unpatentable over Rawson (US 6,128,223) in view of Mitchem (Using Kernel Hypervisors to Secure Applications), in further view of Lettvin (US 5,559,960). As explained below, the rejections are traversed. Reconsideration and withdrawal of the rejections are respectfully requested.

Claims 1, 8 and 15 are generally directed to the initialization of a Virtual Machine Monitor, and the detection of network traffic and physical security intrusion events. More specifically, claims 1, 8, and 15 have been amended to recite the initialization of a plurality of virtual machines, and the identification of specific network traffic and physical security intrusion events. In particular, claims 1, 8, and 15 recite, *inter alia*, initializing a plurality of virtual machines, detecting an incoming network packet, determining whether the incoming network packet is attempting to access a restricted port, performing packet level virus scanning on the network packet, determining whether the incoming network packet is a denial of service attack, and determining whether the incoming network packet is an alert standard format packet. Furthermore, claims 1, 8, and 15 recite, *inter alia*, detecting a physical intrusion, determining whether a user has authorization to initiate the physical intrusion, determining which components of the processor system are vulnerable to the physical intrusion, and disabling the components of the processor system that are vulnerable to the physical intrusion if the user does not have authorization to initiate the physical intrusion.

Claims 1, 8, 15, and 23 were rejected as obvious over Rawson in view of Mitchem, and in further view of Lettvin. However, neither Rawson, Mitchem, nor Lettvin, either alone or in combination, teaches or suggests the initialization of a plurality of virtual machines, the initialization of a virtual machine monitor, or the identification of and the detection of a network intrusion event and a physical intrusion event as recited.

For example, none of Rawson, Mitchem and Lettvin teaches or suggest the initialization of a plurality of virtual machines, and the management of the operation of the virtual machines by the virtual machine monitor. Furthermore, none of Rawson, Mitchem, and Lettvin teaches or suggests the detection of a network packet and the determination of whether the incoming packet is attempting to access a restricted port, the performance of a packet level virus scan, the determination of whether the network packet is a denial of service attack, and the determination of whether the incoming network packet is an alert standard format packet. Finally, none of Rawson, Mitchem, and Lettvin teaches or suggests the detection of a physical intrusion, the determination of which components are vulnerable to the physical intrusion and the disabling of the components that are vulnerable.

In contrast, Rawson is directed to the one time detection of a physical intrusion and fails to teach or suggest the initialization of a virtual machine, a virtual machine monitor, or the detection of a network intrusion. Furthermore, Rawson is limited to a powering off of the entire system once a physical intrusion detection is detected, and fails to teach or suggest the identification of specific components that are vulnerable to the physical intrusion.

Mitchem, meanwhile is directed to using operating system kernel hypervisors to secure applications. Mitchem, as previously noted, describes that the kernel hypervisor is “implemented on top of an operating system kernel,” which, of course, is not a pre-boot phase of

operation. Further, Mitchem merely describes that the hypervisor “is to protect a user, browsing on the Internet, from downloading and executing malicious active contact that might damage the user’s system.” Specifically, the hypervisor accomplishes this by “enforcing a policy that only allowed certain resources [(i.e., files)] to be accessed.” Mitchem, page 179. Furthermore, the hypervisor “does not prevent malicious code from accessing and possibly damaging resources.” Mitchem, page 179. Accordingly, besides being completely silent on the detection of any physical intrusion, Mitchem fails to teach or suggest the detection of a network packet and the determination of whether the incoming packet is attempting to access a restricted port, the performance of a packet level virus scan, the determination of whether the network packet is a denial of service attack, and the determination of whether the incoming network packet is an alert standard format packet.

Finally, Lettvin describes a startup disk that causes a computer to automatically execute a one-time anti-virus software scan each time the computer starts from the disk. Lettvin, however, fails to describe the initialization of a plurality of virtual machines, the initialization of a virtual machine monitor, the detection of a network intrusion, and the detection of a physical intrusion. In particular, Lettvin discloses a virus-resistant disk having a “hidden partition” that initiates a virus scan on startup.

Thus, due to the deficiencies in each of Rawson, Mitchem, and Lettvin, it follows that no combination of the references can render obvious claims 1, 8, 15, or any claims dependent thereon. Accordingly, it is respectfully submitted that all pending claims are in condition for allowance.

Conclusion

If there is any matter that the examiner would like to discuss, the examiner is invited to contact the undersigned representative at the telephone number set forth below.

The Commissioner is hereby authorized to charge any deficiency in the amount enclosed or any additional fees which may be required during the pendency of this application under 37 CFR 1.16 or 37 CFR 1.17 or under other applicable rules to Deposit Account No. 50-2455. Please refund any overpayment to Hanley, Flight, and Zimmerman at the address below.

October 8, 2008

Respectfully submitted,
HANLEY, FLIGHT & ZIMMERMAN, LLC
150 South Wacker Drive, Suite 2100
Chicago, Illinois 60606
/Keith R. Jarosik/
Keith R. Jarosik, Reg. No. 47,683
Attorney for Applicants - (312) 580-1133